Listing of Claims:

1. – 20. (Cancelled).

21. (Currently Amended) A method for authenticating a user for access to at least two entities of a data transmission network via a terminal, each data entity having an associated authentication device, the authentication devices being independent of each other, the method comprising:

a random number is transmitted to the terminal,

a distinct set of data for each of a first entity and a second entity for authenticating the user to both the first and the second entities of the network is calculated by applying ~~using~~ at least one predefined cryptographic algorithm ~~applied~~ to the received random number ~~received~~ using ~~and~~ at least one secret key specific to the user, wherein the distinct set of data comprises (i) a first password for the first entity and (ii) a second password for the second entity,

the terminal inserts, in an access request, first ~~user~~ identifier data and second ~~user~~ identifier data for identifying the user to said first and second entities of the network and the two distinct sets of data,

the terminal transmits the access request to an access controller, wherein the inserted data for authenticating the user comprises a distinct set of data for the first and second entities,

the access controller transmits, to each of the authentication devices for the first and second entities, a respective authentication request containing (i) the first ~~user~~ identifier data and the first password for the first entity, and (ii) the second ~~user~~ identifier data and the second password for the second entity,

the authentication devices of the entities each carry out a user authentication procedure, on the basis of the user identifier data and the respective distinct set of data transmitted to the respective authentication device, and

authentication reports containing results of the authentication procedures carried out by the authentication devices of each of said first and second network entities are transmitted to the terminal.

22. (Previously Presented) The method according to claim 21, characterized in that it includes a preliminary step in which the terminal establishes a connection with a specialized server via the network, wherein the random number is generated and transmitted to the terminal by the specialized server when the connection has been established.

23. (Currently Amended) The method according to claim 22, characterized in that the access request transmitted by the terminal is transmitted to the specialized server which inserts therein the random number used to calculate the authentication data, the access request is then transmitted to the access controller which inserts the random number into the authentication requests transmitted to the authentication devices for the first and second ~~two~~ entities.

24. (Previously Presented) The method according to claim 21, characterized in that the identification data inserted into the access request is in the form: "IdA@DomainA" in which:

"IdA" represents the identifier for identifying the user to the network entity,

"DomainA" represents the identifier of the network entity in the network, with the access controller determining the entities to whom the authentication requests will be transmitted on the basis of the "DomainA" identifiers of the network entity contained in the access request.

25. (Currently Amended) A user terminal capable of accessing, via the access network, at least a first entity and a second entity connected to a data transmission network, each data entity having an associated authentication device, the authentication devices being independent of each other, [[:]] ~~characterized in that it includes~~ the user terminal comprising:

a transmitting apparatus that transmits access requests to the authentication devices for the first and second entities of the network, which requests contain data for identifying and authenticating the user to first and second network entities and each request including user identifier data and a distinct set of data comprising (i) a first password for the first entity and (ii) a second password for the second entity;

a receiving apparatus that receives a random number when a connection with the network is established, a cryptographic calculating apparatus that applies at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to the first and the second entities of the network; [[,]] and

an inserting apparatus that inserts, into each transmitted access request, first ~~user~~ identifier data and second ~~user~~ identifier data for identifying the user to said first and second network entities and calculated authentication data, wherein the calculated authentication data comprises a distinct set of authentication data for the first and second network entities.

26. (Currently Amended) The terminal according to claim 25, further comprising ~~characterized in that it includes~~ an external module designed to be connected to each of the user terminals and including a receiving apparatus that receives the random number from the terminal to which it is connected, a cryptographic calculation apparatus that executes the predefined cryptographic algorithm based on the random number, and for transmitting, to the terminal, at least one data item for authenticating the user to an entity of the network, obtained by the cryptographic calculations.

27. (Currently Amended) An access controller, comprising ~~characterized in that it includes~~ a receiving apparatus that receives a request for access to a first entity and a second entity in a data transmission network coming from a user terminal and transmitted via said network, an extracting apparatus that extracts, from the access request, ~~user~~ first identifier data and second identifier data for identifying and authenticating the user to the first and second network entities, each network entity having an associated authentication device, the authentication devices being independent of each other, wherein the data for authenticating the user to at least the first and second network entities comprises a distinct set of data for each of the network entities, the distinct set of data comprising (i) a first password for the first entity and (ii) a second password for the second entity, a transmitting apparatus that transmits, to each of the authentication devices for the first and second entities, a respective authentication request containing ~~user~~ the first identifier data and the second identifier data for identifying and authenticating the user to a respective one of the first and second entities of the network ~~entity contained~~ included in the access request.

28. (Currently Amended) The access controller according to claim 27, further comprising ~~characterized in that it also includes~~ a receiving apparatus that receives user authentication reports, transmitted by the first and second entities in response to the authentication requests, and a transmitting apparatus that transmits, to the user terminal, an ~~and~~ authentication report based on the reports received from the first and second entities.

29. (Currently Amended) A system for authenticating a user in an attempt to access at least two entities of a data transmission network to which network entities are connected, and which user terminals can access via access networks, ~~characterized in that it includes~~ the system comprising:

a user terminal ~~characterized in that it includes~~ comprising:

a transmitting apparatus that transmits access requests to an entity of the network, which requests contain first ~~user~~ identifier data and second ~~user~~ identifier data for identifying and authenticating the user to first and second entities of the network; and

a receiving apparatus that receives a random number when a connection with the network is established, a cryptographic calculating apparatus that applies at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to the first and second ~~at least two~~ entities of the network and an inserting apparatus that inserts, into each transmitted access request, first ~~user~~ identifier data and second ~~user~~ identifier data and a distinct set of data for each of the first entity and the second entity, wherein the distinct set of data comprises (i) a first password for the first entity and (ii) a second password for the second entity;

at least one authentication server for each of the first and second ~~two~~ network entities, designed to identify and authenticate the users on the basis of the user identifier data and the

respective distinct set of data transmitted to each respective authentication device, the authentication devices being independent of each other;

an access controller comprising ~~characterized in that it includes~~ a receiving apparatus that receives requests for access to the first and second ~~at least two~~ entities of the data transmission network coming from user terminals and transmitted via said network, an extracting apparatus that extracts, from each of the access requests, the data for identifying and authenticating the user to the first and second ~~at least two~~ network entities, a transmitting apparatus that transmits, to each of the ~~two~~ first and second network entities, a respective authentication request containing the data for identifying and authenticating the user to the ~~two~~ first and second network entities, contained in the access request.

30. (Currently Amended) The system according to claim 29, further comprising ~~characterized in that it also includes~~ a specialized server connected to the network so as to be connected to the user terminals when a connection has been established between the terminal and the network, wherein the specialized server includes a generating and transmitting apparatus that generates and transmits a random number to each of the terminals with which a connection is established, and an inserting apparatus that inserts the random number into each of the access requests transmitted by the terminals.

31. (Currently Amended) The system according to claim 29, characterized in that each entity of the network includes a storing apparatus that stores secret keys of users, a determining apparatus that determines the data for authenticating the user to the entity by applying the predefined algorithm to the random number received in a authentication request using ~~and to~~ the

secret ~~user~~ key of the user, and that compares the result obtained to the user authentication data received in the authentication request, wherein the user is properly authenticated by the entity only if the result of the cryptographic calculation obtained is identical to the authentication data contained in the authentication request.